Multidimensional Systems and Signal Processing, 12, 223–251, 2001

Gröbner Bases and Systems Theory

BRUNO BUCHBERGER buchberger@risc.uni-linz.ac.at
Research Institute for Symbolic Computation, Johannes Kepler University, A4040 Linz, Austria

Received April 24, 2001; Revised May 3, 2001

Abstract. We present the basic concepts and results of Gröbner bases theory for readers working or interested in systems theory. The concepts and methods of Gröbner bases theory are presented by examples. No prerequisites, except some notions of elementary mathematics, are necessary for reading this paper. The two main properties of Gröbner bases, the elimination property and the linear independence property, are explained. Most of the many applications of Gröbner bases theory, in particular applications in systems theory, hinge on these two properties. Also, an algorithm based on Gröbner bases for computing complete systems of solutions ("syzygies") for linear diophantine equations with multivariate polynomial coefficients is described. Many fundamental problems of systems theory can be reduced to the problem of syzygies computation.

Key Words: Gröbner bases, algorithmic systems theory, computer algebra, algebraic algorithms, polynomial ideals, elimination, residue class rings, syzygies, polynomial diophantine equations

1. The Purpose of This Paper

This paper is an easy tutorial on Gröbner bases for system theorists who want to know what Gröbner bases are, how they can be computed and how they can be applied.

The theory and computational method of Gröbner bases was introduced in [1, 2] and, since then, has been developed in numerous papers by myself and many others. A recent textbook on the subject is [3], which also contains a complete list of all other, currently available, textbooks on Gröbner bases. Most of these textbooks contain extensive references to the original literature. The Gröbner bases method is also implemented in all major general purpose mathematical software systems like Mathematica, Maple, Derive, etc., see e.g. [4]. There are also a couple of software systems, notably CoCoA [5], Singular [6], and Macaulay [7], that specialize and center around Gröbner bases and put an emphasis both on providing particularly efficient implementations of the Gröbner bases method and related algorithms as well as on covering many of the known applications.

In 1985, N.K. Bose asked me to write a summary chapter on Gröbner bases for his book on n-dimensional systems theory, see [8], because he felt that Gröbner bases might have a rich spectrum of applications in systems theory. This paper stimulated the interest of systems theorists in Gröbner bases. In the seminal paper [9] it then became clear how exactly some fundamental problems of systems theory can be reduced to the problem of constructing Gröbner bases. Meanwhile, quite some papers have been written on this subject and it has been clarified that the following problems of multidimensional and related mathematical systems theory can be essentially reduced to the computation of Gröbner bases, see [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24]:

- factorization of multivariate polynomial matrices,
- solvability test and solution construction of unilateral and bilateral polynomial matrix equations, Bezout identity,
- design of FIR / IIR multidimensional filter banks,
- stabilizability / detectability test and synthesis of feedback stabilizing compensator / asymptotic observer,
- synthesis of deadbeat or asymptotic tracking controller / regulator,
- constructive solution to the nD polynomial matrix completion problem,
- computation of minimal left annhilators / minimal right annhilators,
- elimination of variables for latent variable representation of a behaviour,
- computation of controllable part; controllability test,
- observability test,
- computation of transfer matrix and "minimal realization",
- solution of the Cauchy problem for discrete systems,
- testing for inclusion; addition of behaviors,
- test zero / weak zero / minor primeness,
- finite dimensionality test,
- computation of sets of poles and zeros; polar decomposition,
- achievability by regular interconnection,
- computation of structure indices.

The method of Gröbner bases, originally conceived as a theory and computational method for problems in algebraic geometry, can also be applied to numerous problems in many areas of mathematics other than algebraic geometry and systems theory as, for example, coding theory, integer programming, automated geometric theorem proving, statistics, invariant theory, and formal summation. The proceedings [25] contain tutorials on all these applications.

How is it possible that problems in seemingly so different areas of mathematics can be reduced to the construction of just one mathematical object, namely Gröbner bases? The basic approach is as follows:

A. It often turns out that the formulation of a mathematical problem P involves systems of multivariate polynomials over a commutative coefficient field (or ring), e.g. the field of complex numbers or a finite field. Such problems are potential candidates for trying the Gröbner bases method. The first step then is to find out whether the problem P can be reduced to one of the fundamental problems of algebraic geometry (commutative algebra, polynomial ideal theory), e.g. the problem of deciding the solvability of systems of multivariate polynomial equations, the problem of deciding whether or not a given polynomial is in the ideal generated by a finite set of polynomials, the problem of computing all solutions ("syzygies") of a linear diophantine system of equations with multivariate polynomial coefficients, the problem of computing the Hilbert function of a polynomial ideal, the problem of finding the implicit equation for an algebraic manifold given in parameter presentation etc. In the case of problems P from n-dimensional systems theory this reduction has been provided in papers like [9], see also [10, 11, 12, 14, 16, 17, 18, 19, 20, 21, 22, 23]. Notably, some important problems of systems theory can be reduced to problems in the theory of modules over polynomials and, more specifically, to the computation of syzygies [14, 19, 22, 23].

B. All the problems in algebraic geometry mentioned above and many others have been shown to be reducible, by relatively easy algorithms, to the problem of constructing Gröbner bases. Roughly, this is the following problem: Given a (finite) set F of multivariate polynomials, construct a finite set of polynomials G such that F and G generate the same polynomial ideal and G is in a certain canonical form that, roughly, is a generalization of the triangular form well known for linear multivariate polynomials.

C. Now, the main result of Gröbner bases theory is that the problem of constructing Gröbner bases can be solved algorithmically. Hence, by A. and B., a big variety of problems in mathematics can be reduced to one problem, namely the construction of Gröbner bases, and, since this problem is algorithmically solvable, all these problems can be solved algorithmically. The huge literature on Gröbner bases expands on providing reductions of more and more problems to the problem of constructing Gröbner bases, on improving the algorithmic construction of Gröbner bases, and on generalizing the approach to domains other than polynomial rings over commutative fields, e.g. certain classes of commutative and noncommutative rings.

In this paper, we focus on explaining the essential ideas of B. and C whereas, for A. we have to refer the reader to the specific systems theory literature. We will explain B. and C. by discussing a couple of examples in all detail. We will be able to do this without embarking on formal details and proofs. In fact, it is one of the attractive features of the Gröbner bases method that it is easy to learn how to compute and apply Gröbner bases whereas it is relatively involved to present and understand the underlying theory and the proof of the main theorem, on which the algorithmic construction of Gröbner bases is based. Formal details and a concise version of the proof, whose original form appeared in [1, 2], can be found in [26].

(In other words, in this paper I will present the essentials of Gröbner bases theory in the style of 19th century constructive algebra, when "constructive methods" were mainly described by explaining the methods in typical examples. This style, still, is a good style for making it easy to understand the basic ideas. In contrast, the papers [1, 2] were written in the style of the early sixties, when algorithms and the underlying theory were explicitly formulated but proofs that related algorithms and theorems were given in the usual style of informal mathematics. Later papers by myself, e.g. [26] were, again, written in a different style, which is quite formal and allows formal proofs. I hope that soon, maybe in two or three years' time, I will be able to present the entire theory in such a way that all proofs are automatically generated by our new automated theorem proving system *Theorema*, see [27, 28]. Also, within *Theorema*, it is possible to formulate and execute algorithms so that the world of theorems and proving and the world of algorithms and computing is not separated any more.)

2. Multivariate Polynomial Division (Reduction)

2.1. One Division (Reduction) Step

Consider the set

$$F := \{f_1, f_2\},$$

where

$$f_1 := -3 + 2xy + x^2y$$

$$f_2 := x^2 + xy^2$$

are two bivariate polynomials in the indeterminates x and y, and let

$$h := -x^4 - 3xy + 2x^2y^2.$$

In the above polynomials, the power products $1, x, x^2, \cdots, y, xy, x^2y, \cdots, xy^2, x^2y^2, \cdots$, etc. are ordered lexicographically with the leading power product appearing in the rightmost position. For example, x^2y is the leading power product of f_1 and x^2y^2 is the leading power product of h. The coefficient at the leading power product of a polynomial is called the leading coefficient of the polynomial. Polynomials whose leading coefficient is 1 are called monic. For example, the leading coefficient of h is 2 and both f_1 and f_2 are monic.

Now we execute one "division step" on h using the polynomials in F as divisors, in the following way: We consider the leading power product of h, i.e. x^2y^2, and check whether it is a multiple of the leading power product of any of the polynomials in F. In our example, x^2y^2 is a multiple of x^2y, the leading power product of f_1, namely $x^2y^2{=}y\ (x^2\ \ y)$. Now we subtract $2yf_1$ from h yielding

$$h_1 := -x^4 + 6y - 3xy - 4xy^2.$$

Note that, by this subtraction, the leading power product of h, x^2y^2, disappears and is replaced by monomials whose power products are lower in the lexicographic order. The above procedure is called a "division (or reduction) step". We will also say that h_1 *results from h by one division (or reduction) step modulo F* or that *h reduces to h_1 in one step modulo F.*

2.2. *Division (Reduction) and Cofactors*

The division step can now be repeated: xy^2, the leading power product of h_1, is a multiple of xy^2, the leading power product of f_2, namely $xy^2{=}1\ (xy^2)$. Thus, we subtract $-4\,f_2$ from h_1 yielding

$$h_2 := 4x^2 - x^4 + 6y - 3xy.$$

Note again that, by this operation, the leading power product of h_1 disappears and is replaced by monomials whose power products are lower in the lexicographic order.

Now we are in a situation where no more reduction modulo F is possible: xy, the leading power product of h_2, is neither a multiple of x^2y nor of xy^2, the leading power products of f_1 and f_2, respectively. We say that h_2 *is reduced modulo F.* We also say that h_2 *is a remainder (or a reduced form) of h modulo F.* In fact, *none* of the power products x^2, x^4, y, and xy occurring in h_2 is a multiple of x^2y or xy^2. In such a situation we say that h_2 is *completely reduced modulo F.*

Also note that, by the above procedure, we do not only obtain a Also note that, by the above procedure, we obtain not only a reduced form h_2 of h modulo F but also, as a byproduct, a representation of the form

$$h_2 = h - c_1f_1 - c_2f_2$$

where, in our example, c_1 and c_2 are the two polynomials

$$c_1 := 2y,$$

$$c_2 := -4.$$

We call c_1 and c_2 *cofactors* in the representation of h_2 from h modulo F.

2.3. Remainders (Reduced Forms) are Not Unique

In the example we can observe that, given F and h, there may exist various different sequences of reduction steps that lead to various different reduced forms of h modulo F. In fact, by subtracting $2xf_2$, h also reduces to

$$k_1 := -2x^3 - x^4 - 3xy,$$

which is already in reduced form modulo F.

We advice the reader to compute a couple of reduced forms of polynomials in order to become familiar with this important notion on which all the subsequent notions hinge. For example, consider

$$h := -x^4 - 3x^2y + 2x^3y^2$$

and compute some reduced forms of h modulo the above F together with appropriate cofactors. (One possible sequence of reductions: Subtract, consecutively, $2xyf_1$, $-4xf_2$, and $-3f_1$ from h, yielding the reduced form $-9+4\ x^3-x^4+12xy$. Cofactors: $-3+2xy$ and $-4x$. A different sequence of reductions: Subtract, consecutively, $2xyf_1$, $-4yf_1$, $8f_2$, $-3f_1$, yielding the reduced form $-9-8x^2-x^4-12y+12xy$. Cofactors: $-3-4y+2xy$ and 8.)

2.4. Dependence of Remainders (Reduced Forms) on the Ordering of Power Products

In the above examples, we used the lexicographic ordering of power products determined by stipulating that the indeterminate y ranks higher in the ordering than x. Reduction is also possible w.r.t. many other "admissible" orderings, for example the lexicographic ordering determined by ranking x higher than y or by a "total degree lexicographic ordering" in which power products are, first, ordered by their total degree and lexicographically within a fixed total degree. For example, the ordering $1, x, y, x^2, xy, y^2, x^3, x^2\ y, xy^2, y^3, \cdots$ is a total degree ordering.

(There are infinitely many orderings of power products that are "admissible" for Gröbner bases theory. These orderings can be characterized by two simple axioms. However, in this paper, we do not move to this, more abstract, point of view. The lexicographic and the total degree lexicographic orderings are the ones sufficient for almost all practical purposes.)

It is clear that the leading power products of polynomials, and therefore also the reduced forms of polynomials, change when we change the ordering. For example, the above polynomials f_1, f_2, and h, after ordering their power products by the lexicographic ordering determined by ranking x higher than y, look like this:

$$f_1 = -3 + 2xy + x^2y,$$

$$f_2 = xy^2 + x^2,$$

$$h = -3x^2y + 2x^3y^2 - x^4.$$

Accordingly, a possible reduction of h modulo $F=\{f_1, f_2\}$ may proceed, for example, by subtracting $-x^2\ f_2$, $3\ xyf_1$, $-6yf_1$, and $-3f_1$, yielding the reduced form $-9-18y+15xy+12xy^2$. Cofactors: $-3-6y+3xy$ and $-x^2$. Note that the result is reduced modulo F w.r.t. the lexicographical ordering in which x ranks higher than y but is not reduced modulo F w.r.t. the lexicographic ordering in which y ranks higher than x.

2.5. Exercises Using a Mathematical Software System

Most of the current mathematical software systems provide a built-in function for obtaining one of the reduced forms and the corresponding cofactors of a polynomial h modulo a set of polynomials F w.r.t. various orderings of the power products. For example, in Mathematica this function is called 'PolynomialReduce': When you enter

PolynomialReduce[h, F, $\{y, x\}$]

you obtain the cofactors and the reduced form w.r.t. lexicographic ordering in which y ranks higher than x:

$$\{\{-3 - 4y + 2xy,\ 8\},\ -9 - 8x^2 - x^4 - 12y + 12xy\}.$$

When you enter

PolynomialReduce[h, F , $\{x, y\}$],

you obtain the cofactors and the reduced form w.r.t. lexicographic ordering in which x ranks higher than y:

$$\{\{-3 - 6y + 3xy,\ -x^2\},\ -9 - 18y + 15xy + 12xy^2\}.$$

When you enter

PolynomialReduce[h, F, $\{x, y\}$, MonomialOrder → DegreeLexicographic] you obtain the cofactors and the reduced form w.r.t. total degree lexicographic ordering in which x ranks higher than y:

$$\{\{-3-4y+2xy,\ 8\},\ -9-12y+12xy-8x^2-x^4\}.$$

We suggest that the reader analyzes the individual reduction steps carefully in order to check that, in this example, the reduced form obtained w.r.t. total degree lexicographic ordering with x ranking higher than y is identical to the reduced form obtained w.r.t. lexicographic ordering with y ranking higher than x.

You may also wish to calculate now a couple of examples with n-variate polynomials, $n \geq 3$. For example,

$$\text{PolynomialReduce}[1+xy^3-3xyz^2, \{2+xy+y^2,\ 2x+xyz\},\ \{z,\ y,\ x\}]$$

$$-x^2+xy,\ -3z, 1+2x^2-2xy+x^3y+6xz$$

For studying the rest of the paper, it may be helpful to use a mathematical software system for executing the necessary reductions in the examples.

2.6. *A Subtle Point in the Notion of Reduction*

(This section may be skipped in a first reading. The reader may return to this if he wants to embark on subtle details of the theory.)

We have seen that, if h reduces to r modulo $F=\{f_1,\ldots,f_m\}$, this gives also rise to a representation of the form

$$r = h - \sum_{i=1}^{m} c_i f_i$$

with certain polynomials c_i. However, note that, conversely, not every representation of this form can be interpreted as a reduction, even in case the c_i are monomials. For example, for the F in Section 2.1 and

$$h := xy,$$

$$r := -x^3 - 3y + xy + 2xy^2$$

we have

$$r = h - (-y)f_1 - xf_2$$

but there is no way of reducing h to r modulo F (w.r.t. the lexicographic ordering with y ranking higher than x) because h is already reduced modulo F. In particular, subtracting $-yf_1$ and xf_2 from h is not a possible sequence of reduction steps. (Why not? Answer: The leading power products of $-yf_1$ and xf_2 are not identical to xy, the leading power product of h.)

If you want to start doing proofs for Gröbner bases theory you may try to prove the following lemma: If we have a representation of the above form (in which case we say that r and h are *congruent modulo F*), then there exists a sequence of polynomials $h_1,\cdots,h_k$, such that $h_1=h$, $h_k=r$, and, for all i with $1\leq i<k$, h_i reduces to h_{i+1} in one step modulo F or h_{i+1} reduces to h_i in one step modulo F. In other words, if r and h are congruent modulo F, it may not be possible to go "downwards from h to r" or "downwards from r to h" by reduction steps modulo F but it is always possible to interconnect h and r with reduction steps modulo F that go either "downwards" or "upwards".

(If you feel this lemma or its proof is trivial then you might better check your understanding of the difference between the notion of congruence and the notion of reduction!)

3. Gröbner Bases

3.1. The Notion of Gröbner Bases

Let us now fix some (admissible) ordering of power products. In the examples above we have seen that, modulo a given set F of polynomials, there may exist many different reduced forms of a polynomial h (w.r.t. the admissible ordering considered). Now we define [1, 2]:

A set F of polynomials is called a *Gröbner basis* (w.r.t. the ordering considered) iff all polynomials h have a unique reduced form modulo F.

Example. The above set F is *not* a Gröbner basis w.r.t. the lexicographic ordering that ranks y higher than x: We have seen that, for example, the polynomial $h=-x^4-3xy+2x^2y^2$ has the two distinct reduced forms $4x^2-x^4+6y-3xy$ and $-2x^3-x^4-3xy$.

Example. The set $G=\{9+4x^3+4x^4+x^5, \frac{2}{3}x^2+\frac{1}{3}x^3+y\}$ is a Gröbner basis w.r.t. the same ordering. At the moment, we cannot yet check this. (Note that, for checking this according to the above definition, we would have to consider *infinitely many* polynomials h and their reduced forms!) It is the essential result of Gröbner bases theory that, ultimately, we will be able to provide an *algorithm* for checking whether or not a given finite set of polynomials is a Gröbner basis or not. In fact, this algorithm will also give a handle how to *transform* a set F which is not a Gröbner basis into a Gröbner basis which, in a useful sense, is equivalent to F. For the moment, you may want to try out a couple of reductions of polynomials h to reduced forms modulo G in order to obtain at least a feeling for the uniqueness of these reductions modulo G.

The notion of Gröbner bases can be standardized further [1, 2]:

> A Gröbner basis F is called a *completely reduced Gröbner basis* (w.r.t. the ordering considered) iff all polynomials f in F are monic and are completely reduced modulo $F-\{f\}$.

The above G is a completely reduced Gröbner basis: The coefficients at the leading power products x^5 and y are 1 and $9+4x^3+4\ x^4+x^5$ is completely reduced modulo $\{\frac{2}{3}x^2+\frac{1}{3}x^3+y\}$ (none of the power products of $9+4x^3+4x^4+x^5$ is a multiple of y) and, conversely, $\frac{2}{3}x^2+\frac{1}{3}x^3+y$ is completely reduced modulo $\{9+4\ x^3+4\ x^4+x^5\}$ (none of the power products of $\frac{2}{3}x^2+\frac{1}{3}x^3+y$ is a multiple of x^5).

At first sight it may seem that the uniqueness of reduced forms only concerns a minor side-track of the algebra of multivariate polynomials (commutative algebra, polynomial ideal theory, algebraic geometry). However, it turns out that uniqueness of reduced forms entails a huge number of other nice (useful) properties of Gröbner bases that lay the ground for the algorithmic solution of quite some fundamental problems of this area of algebra. In the sequel, we explain two main properties of Gröbner bases that point into the two main directions of Gröbner bases applications:

- the *elimination property*, which holds for Gröbner bases w.r.t. "elimination orderings", in particular w.r.t. lexicographic orderings of power products, and

- the linear *independence property*, which holds for Gröbner bases w.r.t. arbitrary admissible orderings of power products.

(The elimination property of Gröbner bases was observed first in [29]. The linear independence property was already contained in [1, 2]. The proofs of both properties and many other properties of Gröbner bases based on these two properties are relatively easy.)

3.2. The Elimination Property of Gröbner Bases

First, note that the above example of a Gröbner basis (w.r.t. the lexicographic ordering that ranks y higher than x)

$$\{9+4x^3+4x^4+x^5, \frac{2}{3}x^2+\frac{1}{3}x^3+y\}$$

consists of one univariate polynomial in x and a polynomial in x and y. This is no coincidence but an instance of the general *elimination property* of Gröbner bases w.r.t. lexicographic orderings. Instead of a general formulation of this property let us look to two more examples of (completely reduced) Gröbner bases (w.r.t. lexicographic orderings in which z ranks highest and w ranks lowest):

$$\{-1+x+2x^3-2x^4-2x^6+x^7,\ 1+x^2-2x^3-2x^5+x^6+y,$$

$$-1+x+2x^3-x^4+z\},$$

$$\{-8w-8x+8wx+4x^2-4wx^2-2x^3+x^4,\ -w+w^2-\frac{1}{4}wx^2+wy,$$

$$-x+wx-\frac{1}{4}x^3+xy,\ -\frac{1}{2}wx+wz, -\frac{1}{2}x^2+xz,\ 1-w-y+z^2\}.$$

In practical terms, the elimation property of Gröbner bases (w.r.t. lexicographic orderings of power products) tells us that the polynomials in Gröbner bases introduce the intedeterminates one after the other and that, hence, one can find all the solutions of the algebraic system of equations in Gröbner bases form by solving the system "variable by variable". Let us explain this procedure in the above examples:

The system

$$9+4x^3+4x^4+x^5=0,\ \frac{2}{3}x^2+\frac{1}{3}x^3+y=0$$

described by the first Gröbner basis can be solved by, first, finding all (five) solutions of the univariate polynomial $9+4\ x^3+4x^4+x^5=0$ and, then, for each solution, solving $\frac{2}{3}x^2+\frac{1}{3}x^3+y=0$ for y. Finding the solutions of $9+4x^3+4\ x^4+x^5=0$ exactly and the subsequent exact calculation of y needs algorithms for computing with algebraic numbers. Alternatively, one can find the solutions of $9+4\ x^3+4\ x^4+x^5=0$ numerically and then one also gets an (approximate) value for y from the second equation. Approximations of the five solutions of the first polynomial are

$$\begin{aligned}&\{\ \{x\rightarrow -2.68274\},\\ &\quad\{x\rightarrow -1.3447-1.11887i\},\ \{x\rightarrow 0.686074-0.79095i\},\\ &\quad\{x\rightarrow -1.3447+1.11887i\},\ \{x\rightarrow 0.686074+0.79095i\}\ \}\end{aligned}$$

and the corresponding values for y are then

$$\begin{aligned}&\{1.63791,\\ &\quad -1.24379-0.449783i,\ 0.424835-0.930891i,\\ &\quad -1.24379+0.449783i,\ 0.424835+0.930891i\ \}.\end{aligned}$$

Similarly, the system

$$\begin{aligned}&-1+x+2x^3-2x^4-2x^6+x^7=0,\\ &1+x^2-2x^3-2x^5+x^6+y=0,\\ &-1+x+2x^3-x^4+z=0\end{aligned}$$

described by the second Gröbner basis can be solved by, first, finding all (seven) solutions of the univariate polynomial $-1+x+2x^3-2x^4-2x^6+x^7=0$, then, for each solution x, solving $1+x^2-2x^3-2x^5+x^6+y=0$ for y, and, finally, solving $-1+x+2x^3-x^4+z=0$ for z. Again, doing this exactly needs algorithms for computing with algebraic numbers. Alternatively, one can do this numerically. In fact, in the two Gröbner bases considered so far, the polynomials introducing the indeterminates ranking higher than the indeterminate ranking lowest are all linear in these indeterminates, which makes solving particularly easy. This need not always be the case. The third example reflects the general situation. The system

$$-8w-8x+8wx+4x^2-4wx^2-2x^3+x^4=0,$$

$$-w+w^2-\frac{wx^2}{4}+wy=0,$$

$$-x+wx-\frac{x^3}{4}+xy=0,$$

$$-\frac{wx}{2}+wz=0,$$

$$-\frac{x^2}{2}+xz=0,$$

$$1-w-y+z^2=0$$

has infinitely many solutions: In the Gröbner basis, there does not occur any univariate polynomial in w, the indeterminate with lowest rank. For an arbitrary w, by the elimination property of Gröbner bases, it is guaranteed that we can find a solution x from the first equation. Then we have to solve the second and third equation for y. Again by the elmination property of Gröbner bases, one can be sure that these two simultaneous equations can be solved for y. Even, by the theory of Gröbner bases, one knows that one needs to consider only the nonvanishing equation with lowest degree: For example, taking $w{=}0$, we obtain the four solutions

$$\{\{x\to 0\},\ \{x\to -2i\},\ \{x\to 2i\},\ \{x\to 2\}\}$$

for x. Considering, for example, $x{=}2$, the second and third equations become

$$0=0,$$

$$-2-\frac{8}{4}+2y=0,$$

which yields $y{=}2$. Now the last three equations become

$$0=0,$$

$$-2+2z=0,$$

$$-1+z^2=0.$$

The nonvanishing equation with lowest degree is

$$-2 + 2z = 0,$$

which can be solved for z yielding $z=1$.

For algebraic systems described by Gröbner bases, the above procedure is guaranteed to find *all* solutions.

(For really understanding the essence of the elimination property of Gröbner bases in terms of the possibility of solving the corresponding systems "variable by variable", try the same procedure with a system that is *not* in Gröbner basis form, e.g. the above system

$$-3 + 2xy + x^2y = 0,$$

$$x^2 + xy^2 = 0.$$

Since there is no univariate polynomial in x in the system one might be tempted to believe that for any x a suitable y satisfying both equations can be found. However, this is of course not the case: The condition on y in the first equation may contradict the condition on y in the second equation. For example, trying $x=1$, one obtains the inconsistent conditions

$$-3 + 3y = 0,$$

$$1 + y^2 = 0$$

on y.)

The solution of numerous problems in commutative algebra can now be based on the elimination property, for example the implicitization problem for algebraic manifolds, the decision about the invertibility of polynomial maps, the generation of an ideal basis for the polynomial relations between given polynomials, etc., see [8, 26] and the textbooks on Gröbner bases.

3.3. The Linear Independence Property of Gröbner Bases

The multivariate polynomials over a coefficient field form an associative algebra over this field (i.e. a vector space with a multiplication). The power products constitute a linearly independent basis for this vector space.

Consider now again a set F of polynomials, e.g. the one above. We observe that, for example, $3y$ and $-2x^2-x^3$ are congruent modulo F:

$$3y = -2x^2 - x^3 - yf_1 + xf_2 + 2f_2.$$

In other words, the power products y, x^2, and x^3 are linearly dependent modulo F. In fact, modulo F, there will exist infinitely many linear dependencies between the power products. Now, a fundamental question is how we can obtain a modulo F linearly independent basis consisting of power products. (In the terminology of polynomial ideal theory the question is: How can we obtain a linearly independent basis for the residue class ring modulo the ideal generated by F?) Furthermore, having found a linearly independent basis of the polynomial vector space modulo F, we also want to find the "multiplication table" of the polynomial associative algebra modulo F: For any two power products in the linearly independent vector space basis modulo F we want to find a representation of their product as a linear combination of the basis elements. If we have this information then all questions about the arithmetic modulo F are manageable completely algorithmically.

Now, for Gröbner bases G, this fundamental problem has an easy answer, which we illustrate in the example of the Gröbner basis

$$G = \{x + y^2,\ 3y + 2x^2 + x^3,\ -3 + 2xy + x^2y\},$$

which is a completely reduced Gröbner basis w.r.t. the total degree lexicographic ordering ranking y higher than x. The *linear independence property* of Gröbner bases tells us that exactly the (residue classes represented by those) power products that are not a multiple of any of the leading power products in G form a linearly independent vector space basis (for the residue class ring) modulo F. In our example, these are the power products

$$1, x, y, x^2, xy.$$

Furthermore, the complete multiplication table for these vector space bases elements looks like this

	1	x	y	x^2	xy
1	1	x	y	x^2	xy
x		x^2	xy	$-3y - 2x^2$	$3 - 2xy$
y			y^2	$3 - 2xy$	$-x^2$
x^2				$6y + 4x^2 - 3xy$	$-6 + 3x + 4xy$
xy					$3y + 2x^2$

This means that, for example, the product of the power products x^2 and xy modulo G is $-6+3\,x+4xy$, which is a linear combination of the vector space basis elements 1, x, y, x^2, and xy. The method how we obtain this representation is as follows: We reduce x^2 $(xy)=x^3y$ to (the unique) reduced form modulo G, which can be done by subtracting, subsequently, $y(3y+2x^2+x^3)$, $-2(-3+2xy+x^2y)$, and $-3(x+y^2)$ from x^3y. The resulting reduced form is $-6+3\,x+4xy$.

The solution of numerous problems in commutative algebra can now be based on the linear independence property for Gröbner bases, for example the ideal membership problem, the problem of converting Gröbner bases w.r.t. different orderings of power products, calculation with algebraic numbers, the computation of the Hilbert function of polynomial ideals etc., see [8, 26] and the textbooks on Gröbner bases.

4. The Algorithmic Construction of Gröbner Bases

4.1. The Problem

We have seen that Gröbner bases G have two useful properties that entail numerous other properties on which the algorithmic solution of fundamental problems about G can be based. However, in general, a given set F of polynomials is *not* a Gröbner basis. Thus, the main question is: Is there an *algorithm* by which we can *transform* an arbitrary set F of polynomials into a Gröbner basis G such that G is "equivalent" to F in a way that allows us to pull back the solutions of the fundamental problems on G to solutions of these problems for F.

First of all, we have to define an appropriate notion of equivalence between sets of polynomials:

> Two sets F and G of polynomials (in a fixed number of indeterminates) are called *equivalent* iff the congruence relations determined by F and G are identical, i.e. iff, for all polynomials f and g
>
> f is congruent g modulo F iff f is congruent g modulo G.

(In the language of ideal theory, two sets F and G are equivalent iff they generate the same ideal, i.e. if

$$\{\sum_{i=1}^{m} h_i f_i | m \in \mathbb{N}, h_i \text{ arbitrary polynomials}, f_i \in F\} =$$

$$= \{\sum_{i=1}^{m} h_i g_i | m \in \mathbb{N}, h_i \text{ arbitrary polynomials}, g_i \in G\}.)$$

It is clear that, for equivalent F and G, many of the problems one wants to solve about F are identical or, at least, closely related to the corresponding problems about G. For example, if F and G are equivalent, then the sets of solutions of the algebraic systems determined by F and G (i.e. the algebraic manifolds determined by F and G) are identical. As another example, if F and G are equivalent, then the residue class rings modulo F and G are isomorphic. We will discuss another example, the computation of "syzygies", which turns out to be particularly important for systems theory, in the final section of this paper.

4.2. An Algorithmic Test for Gröbnerianity

Now let us concentrate on the problem of constructing a Gröbner basis G that is equivalent to a given (finite) set F of polynomials. As a first step into this direction, we will solve the following problem:

> Design an algorithm that, given a set F of polynomials, decides whether or not F is a Gröbner basis.

The algorithmic solution for this problem is based on the *main theorem of Gröbner bases theory*. In accordance with the style of this paper, we will focus on explaining the crucial idea behind this theorem on the expense of formal details and proofs: We start with an analysis why a given polynomial set F of polynomials is *not* a Gröbner basis and will gradually reduce the reason why F fails to be a Gröbner basis to *finitely* many, algorithmic, conditions. Checking these finitely many conditions will then establish an algorithm for deciding whether or not a given F is a Gröbner basis.

In the initial example

$$F := \{f_1, f_2\}$$

with

$$f_1 := -3 + 2xy + x^2y$$

$$f_2 := x^2 + xy^2$$

we observed that, for example, the polynomials

$$-x^4 - 3xy + 2x^2y^2$$

and

$$-x^4 - 3x^2y + 2x^3y^2$$

in the lexical ordering with y ranking higher than x, allow reductions modulo F to various distinct normal forms. Now, let us ask ourselves which polynomial is the "simplest" one that, perhaps, reduces to two distinct normal forms modulo F. Apparently, the polynomial

$$x^2y^2$$

which is a pure power product, allows two crucially different initial reduction steps, namely modulo f_1 and modulo f_2 which, perhaps, ultimately will not reduce to the same normal form: By subtracting yf_1, x^2y^2 reduces to

$$h_1 := 3y - 2xy^2.$$

By subtracting xf_2, x^2y^2 reduces to

$$h_2 := -x^3.$$

The polynomial h_2 already is in reduced form modulo G whereas h_1 can be reduced further by subtracting $-2f_2$ yielding

$$2x^2 + 3y$$

as a reduced form modulo F.

Thus, we found that x^2y^2, which in fact is the *least common multiple of the leading power products* of f_1 and f_2, is a witness that the given F is *not* a Gröbner basis because x^2y^2 reduced to at least two distinct reduced forms modulo F. Now, conversely, we may conjecture that if, for a given F, for all $f, g \in F$, all the reductions of the least common multiple of the leading power products of f and g lead to the same reduces form modulo F then F is a Gröbner basis. In fact, this conjecture is true. It is called *the main theorem of the theory of Gröbner bases*. The theorem was conjectured and proved in [1, 2]. The proof is purely combinatorial and relatively involved. A concise version of the proof can be found in [26] and in the textbooks on Gröbner bases. In fact, in [1, 2], we already proved a slightly simpler version of the test for Gröbnerianity: For any reduction algorithm that produces a reduced form of a polynomial h modulo F,

> F is a Gröbner basis iff, for all $f, g \in F$, the reduction of the *S-polynomial* of f and g yields 0.

Here, the S-polynomial of f and g is defined to be the polynomial $u.f-v.g$, where u and v are monomials chosen in such a way that u times the leading monomial of f and v times the leading monomial of g is equal to the least common multiple of the leading power products of f and g. Note that, by construction, the least common multiple of the leading power products of f and g gets cancelled out in the S-polynomial of f and g! (The "S" in "S-polynomial" stands for "Subtraction" referring to the special way of *subtracting* a multiple of g from a multiple of f so that this special *cancellation* of least common multiples of leading power products happens!)

Note also that the above main theorem is true for arbitrary sets F, including infinite sets F. For finite sets F, the above theorem provides an *algorithmic test for Gröbnerianity* because, for testing Gröbnerianity of F, we have to consider a reduction of the *finitely many S-polynomials* of F only instead of considering all the reductions of all *infinitely many polynomials* in the domain of polynomials. Thus, the clue of the main theorem of Gröbner bases theory is that it reduces an infinite test to a finite one.

If we apply the test for the above set F, we obtain one S-polynomial, namely

$$s_{1,2} := yf_1 - xf_2 = -x^3 - 3y + 2xy^2$$

whose reduction modulo F yields

$$-2x^2 - x^3 - 3y.$$

Since the reduced form is not zero we know, by the main theorem, that F is not a Gröbner basis.

Now let us apply the test to an example of a set G which we asserted, in a preceding section, to be a Gröbner basis (w.r.t. the lexicographic ordering of power products in which y ranks higher than x):

$$G := \{g_1, g_2\}$$

with

$$g_1 := 9 + 4x^3 + 4x^4 + x^5,$$

$$g_2 := \frac{2}{3}x^2 + \frac{1}{3}x^3 + y.$$

There are only two polynomials in G. Hence, there is only one S-polynomial:

$$s_{1,2} := yg_1 - x^5 g_2 = -\frac{2}{3}x^7 - \frac{1}{3}x^8 + 9y + 4x^3y + 4x^4y.$$

Reduction of this S-polynomial modulo G yields 0. Hence, G is a Gröbner basis. In fact, we proved in [1, 2] that, for arbitrary f_1 and f_2 with relatively prime leading power products, the reduction of the S-polynomial of f_1 and f_2 modulo f_1, f_2 always yields 0. This fact is called the *product criterion*. In our case, the leading power products of g_1 and g_2 are x^5 and y. They are relatively prime (i.e. their least common multiple is equal to their product). Hence, we need not even execute the reduction of the S-polynomial but can predict, by the product criterion, that the S-polynomial can be reduced to zero and, hence, G is a Gröbner basis.

4.3. Constructing Gröbner Bases

Let us now return to the initial example of a set F of polynomials that is not a Gröbner basis. How can we turn it into an equivalent Gröbner basis? During the test for Gröbnerianity, we have seen that the S-polynomial of the two polynomials f_1 and f_2 of F reduces to the nonzero polynomial

$$-2x^2 - x^3 - 3y.$$

If we adjoin (the monic version of) this polynomial

$$f_3 := \frac{2}{3}x^2 + \frac{1}{3}x^3 + y$$

to F, we obtain a set $\{f_1,f_2,f_3\}$ which has two properties:

- $\{f_1,f_2,f_3\}$ is equivalent to F because f_3 has a presentation of the form

  $$f_3 = c_1 f_1 + c_2 f_2$$

  for certain polynomials c_1 and c_2. This is so because the S-polynomial of f_1 and f_2 is of this form and f_3 results from the S-polynomial by subtracting multiples of f_1 and f_2.

- The S-polynomial of f_1 and f_2 can be trivially reduced to zero modulo $\{f_1,f_2,f_3\}$ because it, first, can be reduced to f_3 using f_1 and f_2 and then, in one step, it can be reduced to zero using f_3.

Now there are two possibilities: Either $\{f_1,f_2,f_3\}$ is already a Gröbner basis in which case, by the main theorem, the reduction of the S-polynomial of f_1 and f_3 and the reduction of the S-polynomial of f_2 and f_3 should yield zero. Or $\{f_1,f_2,f_3\}$ is not a Gröbner basis. In this case, at least one of these two reductions must yield a nonzero polynomial. Let us try this out: We first reduce the S-polynomial of f_1 and f_3 modulo $\{f_1,f_2,f_3\}$ (you may want now to use a mathematical software system for this): The result is the nonzero polynomial

$$f_4 := 9 + 4x^3 + 4x^4 + x^5,$$

which shows that $\{f_1,f_2,f_3\}$ is not yet a Gröbner basis. It is near at hand that we repeat the above step and adjoin the monic polynomial f_4 to $\{f_1,f_2,f_3\}$. Again it is clear that the set $\{f_1,f_2,f_3,f_4\}$ has two properties:

- $\{f_1,f_2,f_3,f_4\}$ is equivalent to F.

- The S-polynomial of f_1 and f_2 and the S-polynomial of f_1 and f_3 can be trivially reduced to zero modulo $\{f_1,f_2,f_3,f_4\}$.

Now we go on in the same way: We check whether the S-polynomial of f_2 and f_3 reduce to zero modulo $\{f_1,f_2,f_3,f_4\}$: This reduction yields zero. Hence, we are left with checking the reduction of the S-polynomial of f_1 and f_4, the S-polynomial of f_2 and f_4, and the S-polynomial of f_3 and f_4: All these reductions yield zero. (In fact, by the product criterion, the last reduction need not be carried out.)

Now we are done: $\{f_1,f_2,f_3,f_4\}$ is a polynomial set that is equivalent to the original set F and, furthermore, all the S-polynomials of $\{f_1,f_2,f_3,f_4\}$ reduce to zero modulo $\{f_1,f_2,f_3,f_4\}$, i.e., by the main theorem, $\{f_1,f_2,f_3,f_4\}$ is a Gröbner basis!

It should be clear how the algorithm goes for arbitrary polynomial sets F. By the main theorem, it should also be clear that the algorithm, if it stops, yields a Gröbner basis that is equivalent to F. For proving that the algorithm terminates for arbitrary input sets F one can either use Hilbert's basis theorem or Dickson's lemma. (The proof based on Dickson's lemma is somewhat nicer because the existence of finite Gröbner bases entails Hilbert's basis theorem.) The above algorithm for constructing Gröbner bases together with its termination proof was introduced also in [1, 2] and constitutes the core of the practical aspect of Gröbner bases theory. (In [1, 2] we also gave a first implementation of the algorithm on a computer and did some first applications, mainly for establishing linearly independent bases for residue classe modulo polynomial ideals and related problems.)

In fact the algorithm can be drastically simplified by a more powerful criterion (the *chain criterion*, which we introduced and proved in [30]) by which, during the execution of the algorithm, the reduction of many of the S-polynomials can be skipped. The chain criterion tells us that the reduction of the S-polynomial of f_i and f_j can be skipped if there exists an f_k such that the leading power product of f_k divides the least common multiple of the leading power products of f_i and f_j and the S-polynomial of f_i and f_k and the S-polynomial of f_k and f_j have already been considered in the algorithm. In the computation above, only the consideration of the S-polynomial of f_2 and f_4 can be skipped by the chain criterion. In more complicated examples, typically, the chain criterion can be applied many times and results in a significant speed-up.

The Gröbner basis obtained above is not yet completely reduced. One can obtain a completely reduced Gröbner basis by reducing each of the polynomials in the Gröbner basis with respect to the other ones. If we do this in our example, it turns out that, in fact, the first two polynomials (i.e. the polynomials which were in the initial set F) reduce to zero and the last two polynomials remain unchanged.

Hence, $G=\{f_3,f_4\}$ is a completely reduced Gröbner basis equivalent to F. In fact, G is the Gröbner basis which we considered as our first example of a Gröbner basis in the section in which we introduced the notion of Gröbner basis. One can prove that completely reduced Gröbner bases are uniquely determined by the ideal generated by them. In other words, given an F there is exactly one completely reduced Gröbner basis equivalent to F. (All this is of course only true w.r.t. a fixed admissible ordering of the power products. Given an F, in general, there may exist various different completely reduced Gröbner bases equivalent to F. It is a nontrivial fact that, actually, for a given F there exist only finitely many different completely reduced Gröbner bases - although there exist infinitely many different admissible orderings of power products! For this surprising result see, for example, the textbook [3].)

In fact, as a strategy during the construction of a Gröbner basis, it is much better to keep already the intermediate bases (completely) reduced rather than waiting with the complete reduction until the termination of the algorithm. The construction of Gröbner bases is a task that can be shown to be inherently complex. Considerable effort has been made to come up with improved versions of the algorithm. For recent progress see the textbooks and the original literature cited in the textbooks. One of the main new ideas is what is called the "Gröbner walk". In this version of the algorithm, one first computes the Gröbner basis of a given F using the above algorithm w.r.t. a total degree lexicographic ordering. It is known that the algorithm tends to have shortest computing times w.r.t. these ordering. Then one "walks" from the Gröbner basis with respect to such an ordering to the

Gröbner basis w.r.t. the desired ordering in incremental steps whose sequence is determined, roughly, by the topology of the admissible orderings.

You may want now to study, for a fixed F, the corresponding completely reduced Gröbner basis w.r.t. various admissible orderings. For this, you may now use the implementation of the above algorithm, which is available in all current mathematical software systems. For example, in Mathematica, the algorithm can be called by the name ‘GroebnerBasis’. Again the ordering of power products to be used can be indicated by extra arguments to the function:

$$
\begin{aligned}
\text{In}[1] \quad &:= \text{GroebnerBasis}[\{xyz - x^2y - 1,\, x^2 - yz,\, y^2 - x\},\, \{x, y, z\}] \\
\text{Out}[1] \quad &:= \{1 - 3z^2 + 3z^4 + z^5 - z^6, y - z + z^2 + 2z^3 + z^4 - z^5, \\
&\quad\ x + 2z - 3z^3 - z^4 + z^5\} \\
\text{In}[2] \quad &:= \text{GroebnerBasis}[\{xyz - x^2y - 1,\, x^2 - yz,\, y^2 - x\},\, \{z, y, x\}] \\
\text{Out}[2] \quad &:= \{-1 + 2x^3 + x^5 - x^6,\, x + x^3 - x^4 + y,\, -x^2 - x^4 + x^5 - z\} \\
\text{In}[3] \quad &:= \text{GroebnerBasis}[\{xyz - x^2y - 1,\, x^2 - yz,\, y^2 - x\},\, \{z, y, x\}, \\
&\quad\ \text{MonomialOrder} \rightarrow \text{DegreeLexicographic}] \\
\text{Out}[3] \quad &:= \{-xy + z,\, -x + y^2,\, x^2 - yz,\, 1 + xz - z^2,\, 1 - x^3 + xz,\, 1 + y + xz - x^2z\}
\end{aligned}
$$

4.4. Computing Gröbner Bases with Cofactors

If, in the above algorithm for constructing Gröbner bases, we keep track of the reductions necessary for producing the polynomials in the Gröbner basis G from the initial polynomials in F we obtain important additional information, which will be essential for the application of Gröbner bases to syzygy computations, a topic in the center of interest for systems theory based on module theory.

Again, we explain this in our initial example:

$$F = \{f_1, f_2\}$$

where

$$
\begin{aligned}
f_1 &= -3 + 2xy + x^2y, \\
f_2 &= x^2 + xy^2.
\end{aligned}
$$

As explained above, the first S-polynomial

$$s_{1,2} := yf_1 - xf_2 = -x^3 - 3y + 2xy^2$$

is a linear combination of f_1 and f_2. By reduction modulo $\{f_1, f_2\}$ we obtain the polynomial f_3 which, after making it monic by multiplication by $-\frac{1}{3}$, will then be the first polynomial in the corresponding Gröbner basis. From the explicit information on the cofactors in the reduction we obtain the representation of f_3 as a linear combination of f_1 and f_2:

$$f_3 = -\frac{1}{3}yf_1 + \left(\frac{2}{3} + \frac{1}{3}x\right)f_2.$$

Similarly, we can obtain a representation of of f_4 as a linear combination of f_1 and f_2: First, we compute the S-polynomial $s_{1,3}$ of f_1 and f_3:

$$s_{1,3} := f_1 - x^2 f_3 = -3 - \frac{2}{3}x^4 - \frac{1}{3}x^5 + 2xy.$$

Now, we reduce $s_{1,3}$ modulo $\{f_1, f_2, f_3\}$ obtaining

$$-3 - \frac{4}{3}x^3 - \frac{4}{3}x^4 - \frac{1}{3}x^5.$$

We make this polynomial monic by multiplication by -3 and obtain as the next polynomial in the Gröbner basis

$$f_4 := 9 + 4x^3 + 4x^4 + x^5.$$

Using the information on cofactors in the reduction, we obtain a representation of f_4 as a linear combination of f_1, f_2, and f_3:

$$f_4 = (-3)f_1 + (3x^2 + 6x)f_3.$$

If we plug into this the representation of f_3 in terms of f_1 and f_2, we finally obtain a representation of f_4 in terms of the original f_1 and f_2:

$$f_4 = (-3 - 2xy - x^2y)f_1 + (4x + 4x^2 + x^3)f_2.$$

Summarizing, in the course of constructing the Gröbner basis

$$G := \{g_1, g_2\}$$

where

$$g_1 := f_3,$$

$$g_2 := f_4,$$

by keeping track of the cofactors in the reductions, we can establish a transformation matrix U

$$U := \begin{pmatrix} -\frac{1}{3}y & \frac{2}{3} + \frac{1}{3}x \\ -3 - 2xy - x^2y & 4x + 4x^2 + x^3 \end{pmatrix}$$

such that, in a somewhat sloppy notation,

$$G = U.F.$$

The Gröbner basis algorithm that also computes the transformation matrix U is called the "extended Gröbner basis algorithm". Unfortunately, some of the current mathematical software systems (including Mathematica) only contain implementations of the Gröbner basis algorithm that display the final Gröbner basis and "throw away" the intermediate information that could be used for constructing, with basically no extra effort, the transformation matrix U.

One also can construct a reverse transformation matrix V such that

$$F = V.G.$$

In fact, the construction of V is conceptionally much easier than the construction of U. We will explain the construction as a byproduct in the next section.

5. The Computation of Syzygies Using Gröbner Bases

5.1. One Inhomogeneous Linear Diophantine Equation with Polynomial Coefficients

Let us consider the following problem: Given again

$$f_1 := -3 + 2xy + x^2y$$

$$f_2 := x^2 + xy^2$$

and the polynomial

$$h := \frac{2}{3}x^2 + \frac{1}{3}x^4 + xy,$$

find p_1 and p_2 such that

$$f_1p_1 + f_2p_2 = h.$$

Such an equation is called an inhomogenous linear diophantine equation in the ring of (bivariate) polynomials.

Having the Gröbner bases method at our disposition, this problem can now be solved easily: We first compute the corresponding Gröbner G corresponding to $F = \{f_1, f_2\}$ (w.r.t. any admissible ordering, e.g. the lexicographic ordering that ranks y higher than x). We already did this in the previous sections:

$$G = \{g_1, g_2\}$$

with

$$g_1 := \frac{2}{3}x^2 + \frac{1}{3}x^3 + y,$$

$$g_2 := 9 + 4x^3 + 4x^4 + x^5.$$

Now, since F and G are equivalent (i.e. generate the same ideal), h has a representation of the form

$$f_1 p_1 + f_2 p_2 = h \tag{A1}$$

iff it has a representation of the form

$$g_1 q_1 + g_2 q_2 = h. \tag{B1}$$

By one of the fundamental properties of Gröbner bases (which is an easy consequence of the linear independence property of Gröbner bases), the existence of q_1 and q_2 such that (B1) holds can be decided by reducing h to a reduced form modulo G: The reduced form of h modulo G is

$$\frac{2}{3}x^2 - \frac{2}{3}x^3.$$

Since this polynomial is nonzero, we know that the equation (B1) and, hence, equation (A1) has no solution. (Note that, we cannot decide (A1) directly by reducing h modulo F: The reduced form of h modulo F is h, i.e. a nonzero polynomial. However, since F is not a Gröbner basis, we cannot infer from this that no solution to (A1) exists!)

Now let us look to

$$h := -x^3 - 3y + 2xy^2.$$

Reduction of h modulo G yields 0. Thus, we know that (B1), and hence also (A1), has a solution. By the reduction of h modulo G we obtain the cofactor representation:

$$h = q_1 g_1 + q_2 g_2$$

with

$$q_1 := 2xy - \frac{2}{3}x^4 - \frac{4}{3}x^3 - 3,$$

$$q_2 := \frac{2}{9}x^2.$$

Now, using the transformation matrix U of the previous section, we obtain a representation of h in terms of f_1 and f_2:

$$h = (q_1\ q_2).\begin{pmatrix} g_1 \\ g_2 \end{pmatrix} = (q_1\ q_2).U.\begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = (p_1\ p_2).\begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$$

with

$$p_1 := -\frac{2}{3}x^2 + y - \frac{2}{3}xy^2$$

$$p_2 := -2 - x + \frac{4}{3}xy + \frac{2}{3}x^2y.$$

Summarizing, using Gröbner bases, we can always decide the solvability of an inhomogeneous linear diophantine equation with multivariate polynomial coefficients and, in the case that a solution exists, obtain one special solution. How about the general solution? We will discuss this problem and its solution by Gröbner bases in the next section.

Note that, by the reduction of polynomials modulo G, one can easily calculate also a matrix V such that

$$F = V.G,$$

i.e. the original polynomial set F can be obtain as a linear combination of the polynomials in the corresponding Gröbner basis G. For this, we only have to reduce the polynomials f_1 and f_2 modulo G, which must yield 0 because G is a Gröbner basis and f_1 and f_2 are in the ideal generated by G. By doing this and collecting the cofactors, we obtain

$$f_1 = (2x + x^2)g_1 + \left(-\frac{1}{3}\right)g_2,$$

$$f_2 = \left(-\frac{2}{3}x^3 - \frac{1}{3}x^4 + xy\right)g_1 + \left(\frac{1}{9}x^2\right)g_2.$$

Hence,

$$V := \begin{pmatrix} 2x + x^2 & -\frac{1}{3} \\ -\frac{2}{3}x^3 - \frac{1}{3}x^4 + xy & \frac{1}{9}x^2 \end{pmatrix}$$

is the desired matrix.

5.2. One Homogeneous Linear Diophantine Equation with Polynomial Coefficients

Now let us study the homogeneous case. Given, again,

$$f_1 := -3 + 2xy + x^2y$$
$$f_2 := x^2 + xy^2$$

we want to find (all) pairs of polynomials p_1 and p_2 such that

$$f_1p_1 + f_2p_2 = 0. \tag{A2}$$

Again, we first compute the Gröbner basis G corresponding to $F = \{f_1, f_2\}$ (w.r.t. any admissible ordering, e.g. the lexicographic ordering that ranks y higher than x) and study the homogeneous linear equation

$$g_1q_1 + g_2q_2 = 0. \tag{B2}$$

Now the S-polynomials turn out to play a fundamental role that goes beyond the construction of the Gröbner basis. Namely, it can be proved that the reduction of the S-polynomial of g_1 and g_2 gives rise to a solution $(\bar{q}_1, \bar{q}_2)$ and that all the infinitely many other solutions can be obtained in the form $c.(\bar{q}_1, \bar{q}_2)$ with an arbitrary polynomial c: We first compute the S-polynomial

$$t_{1,2} := x^5g_1 - yg_2 = \frac{2}{3}x^7 + \frac{1}{3}x^8 - 9y - 4x^3y - 4x^4y.$$

Now, we reduce $t_{1,2}$ to a reduced form modulo G, which necessarily must be zero. By keeping track of the cofactors in the reduction we see that

$$(x^5g_1 - yg_2) - (-9 - 4x^3 - 4x^4)g_1 - \left(\frac{2}{3}x^2 + \frac{1}{3}x^3\right)g_2 = 0.$$

Hence,

$$\overline{q_1} := +9 + 4x^3 + 4x^4 + x^5,$$

$$\overline{q_2} := -\frac{2}{3}x^2 - \frac{1}{3}x^3 - y$$

is a possible solution for (B2). Using the matrix U, the solutions can now again be transformed back to (all) solutions of (A2).

In the general case of an equation

$$g_1 q_1 + \ldots + g_m q_m = 0$$

where $\{g_1, \cdots, g_m\}$ is a Gröbner basis in a multivariate polynomial ring, the reduction of the $m.(m-1)/2$ many S-polynomials to zero establish $m.(m-1)/2$ many solutions $(q_1, \cdots, q_m)$ of the equation. It can be shown that the infinitely many other solutions can be obtained by linear combination of these solutions with arbitrary polynomial factors.

5.3. Several Linear Diophantine Equations with Polynomial Coefficients

The case of finitely many linear diophantine equations can either be reduced to the case of just one such equation (by introducing slack variables) or one can develop the entire theory of Gröbner bases over the domain of modules over a multivariate polynomial ring. The latter approach appears to be more natural. No essentially new ideas are necessary for doing this, see the textbooks on Gröbner bases, notably [3].

Being able to obtain a finite basis for the entire module of the infinitely many solutions to a system of linear diophantine equations in the ring of multivariate polynomials is now the clue to an algorithmic solution to some of the fundamental problems of systems theory listed in the first section of this paper, see [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24].

6. Conclusion

We gave an introduction to the key ideas and techniques of Gröbner bases theory such that the reader should now be able to compute Gröbner bases and to compute solutions to the most important problems that can be solved by Gröbner bases and on which a whole cascade of problems hinges in many areas of mathematics, in particular systems theory. The reader should now also be able to use the implementations of my algorithm for computing Gröbner bases, which by now is available as a built-in function in all current mathematical software systems like Mathematica, Maple, Macsyma, Mupad, Derive, Magma. If the reader wants to go into experimenting with more sophisticated applications, we advice him to use specialized systems like CoCoA, Singular, and Macaulay. If you want to embark on the theory and the investigation of possibly new applications in the area of systems theory, you should consult the textbooks on Gröbner bases listed in [3] and, finally, the original literature cited in these textbooks and, in particular, e.g. [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24]. If you find new applications, please, let me know: Buchberger@RISC.Uni-Linz.ac.at.

Acknowledgments

Work on this paper was supported by Project 1302 of the Austrian Science Foundation (FWF). I would also like to thank the editors Zhiping Lin and Li Xu for their encouragement and, in particular, valuable help with the references. Finally, my best thanks go to my PhD students Koji Nakagawa and Wolfgang Windsteiger for proof-reading and technical help.

References

1. B. Buchberger, *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal(German)*, Phd thesis, Univ. of Innsbruck (Austria), 1965.
2. B. Buchberger, "An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations (German)," *Aequationes Mathematicae*, vol. 4, no. 3, 1970, pp. 374–383. English translation in [25].
3. M. Kreuzer, and L. Robbiano, *Computational Commutative Algebra I*, Springer Verlag, New York, 2000.
4. S. Wolfram, *The Mathematica Book*, Cambridge University Press and Wolfram Research, Inc., New York, NY, USA and 100 Trade Center Drive, Champaign, IL 61820-7237, USA, fourth edition, 1999.
5. A. Capani, G. Niesi, and L. Robbiano, *CoCoA, A System for Doing Computations in Commuatative Algebra*, 1998, Available via anonymous ftp from cocoa.dima.uniqe.it.
6. G.-M. Greuel, G. Pfister, and H. Schönemann, *Singular Reference Manual*, Reports On Computer Algebra, number 12, Centre for Computer Algebra, University of Kaiserslautern, 1997, http://www.mathematik.uni-kl.de/~zca/Singular.
7. D. Grayson, and M. Stillman, *Macaulay 2: A Software System for Algebraic Geometry and Commutative Algebra*, Available over the web at http://www.math.uiuc.edu/Macaulay2.
8. B. Buchberger, "Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory," In N. K. Bose (Ed.), *Multidimensional Systems Theory,* Dodrecht: Reidel Publishing Company, 1985, chapter 6, pp. 184–232.
9. U. Oberst, Multidimensional Constant Linear Systems, *Acta Applicandae Mathematicae*, vol. 20, 1990, pp. 1–175.
10. J. P. Guiver, and N. K. Bose, "Causal and Weakly Causal 2-D Filters with Applications in Stabilization," In N. K. Bose (Ed.), *Multidimensional System Theory*, Dordrecht: Reidel, 1985, p. 52.
11. E. Fornasini, "A Note on Output Feedback Stabilizability of Multivariable 2D Systems," *Systems & Control Letters*, vol. 10, 1998, pp. 45–50.
12. L. Xu, O. Saito, and K. Abe, "Bilateral Polynomial Matrix Equation in Two Indeterminates," *Multidimensional Systems and Signal Processing*, vol. 1, no. 4, 1990, pp. 363–379.
13. A. Logar, and B. Sturmfels, "Algorithms for the Quillen-Suslin Theorem," *J. Algebra*, vol. 145, 1992, pp. 231–239.
14. L. Xu, O. Saito, and K. Abe, "Output Feedback Stabilizability and Stabilization Algorithms for 2D Systems," *Multidimensional Systems and Signal Processing*, vol. 5, 1994, pp. 41–60.
15. H. Park, and C. Woodburn, "An Algorithmic Proof of Suslin's Stability Theorem for Polynomial Rings," *J. Algebra*, vol. 178, 1995, pp. 277–298.
16. H. Park, T. Kalker, and M. Vetterli, "Gröbner Bases and Multidimensional FIR Multirate Systems," *Multidimensional Systems and Signal Processing*, vol. 8, no. 1/2, 1997, pp. 11–30.

17. L. Xu, J. Q. Ying, and O. Saito, "Feedback Stabilization for a Class of MIMO nD Systems by Gröbner Basis Approach," In *Abstract of First International Workshop on Multidimensional Systems*, Poland, 1998, pp. 88–90.
18. S. Basu, "Multi-dimensional Filter Banks and Wavelets – A System Theoretic Perspective," *J. Franklin Inst.*, vol. 335B, no. 8, 1998, pp. 1367–1409.
19. N. K. Bose, and C. Charoenlarpnopparut, "Multivariate Matrix Factorization: New Results," In *Mathematical Theory of Networks and Systems, Proceedings of MTNS-98*, Podova, Italy, 1998, pp. 97–100.
20. C. Charoenlarpnopparut, and N. K. Bose, "Multidimensional Filter Bank Design Using Gröbner Bases," *IEEE Trans. on circuits and Systems II: Analog and Digital Signal Processing*, vol. 46, December 1999, pp. 1475–1486.
21. H. Pillai, J. Wood, and E. Rogers, "Gröbner Bases and Constructive Multidimensional Behavioural Theory," In *Proc. of the Second International Workshop on Multidimensional Systems*, Poland, 2000, pp. 83–89.
22. Z. Lin, On Syzygy Modules for Polynomial Matrices, *Liner Algebra and Its Applications*, vol. 298, 1999, pp. 73–86.
23. Z. Lin, "Output Feedback Stabilizability and Stabilization of Linear *n*-D Systems," In *Multidimensional Signals, Circuits and Systems*, Taylor & Francis, 2001, chapter 4, pp. 59–76.
24. J. Wood, "Modules and Behaviours in nD Systems Theory," *Multidimensional Systems and Signal Processing*, vol. 11, 2000, pp. 11–48.
25. B. Buchberger, and F. Winkler, eds. *Gröbner Bases and Applications*, volume 251 of *London Mathematical Society Series*. Proc. of the International Conference "33 Years of Groebner Bases." Cambridge University Press, 1998.
26. B. Buchberger, *Introduction to Gröbner Bases*, Cambridge University Press, 1998, pp. 3–31 in [25].
27. B. Buchberger, T. Jebelean, F. Kriftner, M. Marin, E. Tomuţa and D. Văsaru, "A Survey on the Theorema Project," In Wolfgang W. Küchlin (ed.), *Proceedings of ISSAC '97(the 1997 International Symposium on Symbolic and Algebraic Computation)*, July 21–23, 1997, Maui, Hawaii, ACM Press, pp. 384–391, 1997.
28. B. Buchberger, C. Dupré, T. Jebelean, F. Kriftner, K. Nakagawa, D. Văsaru and W. Windsteiger, "The Theorema Project: A Progress Report," In M. Kerber and M. Kohlhase (eds.), *8th Symposium on the Integration of Symbolic Computation and Mechanized Reasoning*, St. Andrews, Scotland, August 6–7, Universität des Saarlandes, Germany, 2000, pp. 100–115.
29. W. Trinks, "On B. Buchberger's Method for Solving Systems of Algebraic Equations," *J. Number Theory*, vol. 10. no. 4, 1978, pp. 475–488.
30. B. Buchberger, A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases, In Edward W. Ng, editor, *Proceedings of the International Symposium on Symbolic and Algebraic Manipulation (EUROSAM '79)*, Marseille, France, volume 72 of *Lecture Notes in Computer Science*, Springer, 1979, pp. 3–21.